EXPRESS MAIL NO. EV 286 259 342 US

Docket No. 03AB087

110003.00034

PATENT APPLICATION FOR

SAFETY CONTROLLER WITH SAFETY RESPONSE TIME MONITORING

by

ANTHONY GERARD GIBART

SAFETY CONTROLLER WITH SAFETY RESPONSE TIME MONITORING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] --

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0002] --

BACKGROUND OF THE INVENTION

[0003] The present invention relates to industrial controllers used for real-time control of industrial processes, and in particular to "high reliability" or "safety" industrial controllers appropriate for use in devices or with devices intended to protect human life and health.

[0004] Industrial controllers are special-purpose computers used in controlling industrial processes. Under the direction of a stored, controlled program, an industrial controller examines a series of inputs reflecting the status of the controlled process and changes a series of outputs controlling the industrial process. The inputs and outputs may be binary, that is, on or off, or analog, providing a value within a substantially continuous range. The inputs may be obtained from sensors attached to the controlled process, and the outputs may be signals to actuators on the controlled process.

[0005] "Safety systems" are systems intended to ensure the safety of humans working in the environment of an industrial process. Such systems may include the electronics associated with emergency-stop buttons, light curtains, and other machine lockouts. Traditionally, safety systems have been implemented by a set of redundant circuits separate from the industrial control system used to control the industrial process with which the safety system is associated. Such safety systems have been "hardwired" from switches and relays including specialized "safety relays" which provide comparison of redundant signals and internal checking of fault conditions such as welded or stuck contacts.

[0006] Hard-wired safety systems using duplicate wiring have proven cumbersome in practice, in part because of the difficulty of installing and connecting hardwired components and duplicate sets of wiring, particularly in complex control applications, and in part because of the difficulty of troubleshooting and maintaining a hard-wired system whose logic can be changed only by re-wiring.

[0007] For this reason, there has been considerable interest in developing industrial controllers that may implement safety systems using a program simulating the operation of the physical components in hard-wired safety systems. Industrial controllers are not only easier to program but may provide reduced installation costs by eliminating long runs of redundant wiring in favor of a high speed serial communication network and by providing improved troubleshooting capabilities. U.S. Patent applications 60/373,592 filed April 18, 2002; 10/034,387 filed December 27, 2001; 09/667,145 filed September 21, 2000; 09/666,438 filed September 21, 2000; and 09/663,824 filed September 18, 2000, assigned to the assignee of the present invention, describe the implementation of safety systems using industrial controller architectures, and are hereby incorporated by reference.

[0008] When an industrial controller is used to implement a safety process in lieu of hard-wired devices, it is important that the speed of propagation of safety signals through the components of the industrial controller is well characterized. Importantly, safety processes requiring response speeds that exceed those possible with the industrial controller, because of signal propagation delay, must be avoided.

[0009] The propagation delay of a given signal through an industrial controller will vary as a function of network loading, computational complexity, and other often unknown factors. For this reason, the propagation delay of an industrial controller is normally characterized by summing the worst-case delays of each of the components of the industrial controller in the signal chain from input circuit through processor to the output circuit. Each of these components may also have a watchdog timer ensuring that the delay at the component does not exceed this worst case delay value and notifying the user and entering a safety state should this restraint be violated by any given signal.

[0010] Worst-case delay values must be conservatively estimated and therefore, when they are added together, the total worst case delay is substantially longer than the typical propagation delay of the industrial controller. Further because there is some statistical independence in the actual propagation delays at the components, worst-case delays at some components, will typically be offset by lesser delays at other components. Nevertheless, a simple summing of worst-case delay values is used because actual propagation delay of a given signal is known only too late to avoid unsafe operation.

SUMMARY OF THE INVENTION

[0011] The present inventor has recognized that although the actual propagation delay of each signal cannot be known before the signal has arrived at the output circuits, the signal's current propagation time since inception can be determined and compared to a threshold value that may be set significantly beneath the sum of the worst-case propagation delays of the components. When the current propagation time exceeds this threshold, a safety state can be entered even before the signal has fully propagated. In this way, the industrial controller can be used for safety applications requiring higher speeds than would be suggested by the worst-case propagation delay of the industrial controller.

[0012] Specifically, the present invention provides a safety industrial controller receiving signals from electrical sensors on a safety process and providing signals to electrical actuators on the safety process. The safety industrial controller includes input circuits receiving input signals from sensors and transmitting them to logic circuitry before a first worst-case delay. Logic circuitry receives the input signals from the input circuits to create at least one output signal based on the input signals and transmits the output signal to an output circuit before a second worst case delay. Output circuitry receiving the output signal from the logic circuitry outputs the output signal to an actuator before a third worst case delay only if the time elapsed since the input circuits received at least one input signal is less than a predetermined time limit less than the sum of the first, second, and third worst case delays. Otherwise, the output circuit enters a predetermined safety state.

[0013] It is thus one object of the invention to provide a monitoring of ongoing propagation delay that may be used to permit an industrial controller to implement safety systems requiring a higher response speed than would be indicated by the industrial controller's worst case propagation delay.

[0014] The input circuit may repeatedly transmit the input signals to the logic circuitry at a predetermined period less than the predetermined time period, and the logic circuitry may create the output signal at a repetition rate triggered by the receipt of the input signals.

[0015] Thus, it is one object of the invention to provide a simple mechanism for monitoring the accumulating propagation delay in signals passing through the industrial controller by regularly repeating the input signal.

[0016] The input circuitry may include a time stamp means creating a time stamp indicating a time corresponding to the receiving of the input signals by the input circuits. The logic circuitry may include a means for associating the output signal with one time stamp of the input signals so received, and the output circuitry may provide an output signal to an actuator only when the output signal arrives at the output circuit before a time equal to a time stamp associated with a previous output signal plus a predetermined time limit.

[0017] Thus it is another object of the invention to provide a mechanism for determining accumulating propagation delay that can detect even slow increases in propagation delay.

[0018] The association of the output signal with one time stamp may, in a simple case, take the earliest time stamp of the input signal so received. Alternatively, the association may follow a user-defined time stamp function indicating which of the time stamps of the input signal is forwarded by the output signal.

[0019] It is thus another object of the invention to provide a method of propagating a time stamp through a complex control execution thread in which multiple time-stamped input signals become one time stamped output signal.

[0020] The worst-case delays may include network transmission times between input and logic circuits and output and logic circuits.

[0021] Thus it is another object of the invention to provide a monitoring of propagation delays that works with networked systems.

[0022] The predetermined time limit may be greater than the sum of average delays associated with the worst-case delays.

[0023] Thus it is another object of the invention to provide a mechanism which does not enter a safety state unnecessarily at slight variations in propagation delay time.

[0024] The input and output circuits may have synchronized clocks or may have asynchronous clocks and the input circuit may provide a value to the output circuit indicating an offset between the clocks of the input and output circuits. In this latter case, the predetermined time limit may take into account the offset value and any uncertainty in the offset value.

[0025] Thus it is another object of the invention to provide a simple method for use with synchronized clock systems but that also works with asynchronous clock systems of arbitrary precision.

[0026] These particular objects and advantages may apply to only some embodiments falling within the claims and thus do not define the scope of the invention.

BRIEF DESCRIPTION OF THE FIGURES

[0027] Fig. 1 is a simplified perspective view of a control system suitable for use with the present invention receiving redundant signals from a light curtain to lock operation of a press protected by the light curtain;

[0028] Fig. 2 is a block diagram of the components of the control system of Fig. 1 showing the redundant light curtain signals as received by input circuitry on an input module to be transmitted along a backplane to a logic module providing signals transmitted in turn along the backplane to an output module ultimately to be provided to an actuator on the press through output interface circuitry;

[0029] Fig. 3 is a representation of the signal path and components of Fig. 2 showing the definition of several worst case and average delays;

[0030] Fig. 4 is a schematic representation of the processing of input time stamps as implemented by the logic processor of Fig. 2 for associating a time stamp with an output signal generated from numerous input signals; and

[0031] Fig. 5 is a flow chart of a program executed by the output circuit based on its receipt of safety signals.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0032] "High reliability" and "safety" systems are those that guard against the propagation of erroneous data or signals by detecting error or fault conditions and signaling their occurrence and/or entering into a predetermined fault state. High reliability systems may be distinguished from high availability systems which attempt to remain operating after some level of failure. The present invention may be useful in both systems, however, and therefore, as used herein, high reliability and safety should not be considered to exclude high availability systems that provide safety operation.

[0033] Referring now to Fig. 1, a safety controller 10 may include generally a plurality of modules 12 held in a rack 14 for intercommunication along a backplane 16, the backplane 16 providing an electrical channel of communication between the modules 12. Alternatively, the backplane may be any generalized serial communication network.

[0034] The modules 12 may include a power supply module 18 providing power to the other modules 12, one or more processor modules 20 providing logical processing of received signals according to control programs (not shown) executed by contained microprocessors, and input/output (I/O) modules 22 which may receive electrical signals from or transmit electrical signals to a safety process 24.

[0035] In a present example, the safety process 24 includes a light curtain 26 providing redundant light curtain signals 28 to an input I/O module 22 and a press 30 that may be stopped via halt signal 32 to the press 30 provided from output I/O module 22'. The safety process 24 is intended to stop the press 30 if the light curtain is broken. A speed of response of the safety controller 10 in halting the press 30 after breaking of the light curtain 26 determines the necessary amount of separation required between the light curtain 26 and the press 30. Large separation between the

light curtain 26 and the press 30, necessitated by undue delay in the response of the safety controller 10, may hamper practical use of the press 30 must be avoided.

[0036] Referring now to Figs. 2 and 3, the safety controller 10 receives redundant light curtain signals 28 (indicating that the light curtain 26 is broken) at input interface circuitry 33. The input interface circuitry provide for input filtering of these electrical signals to eliminate noise and the like, as is known in the art. This filtering introduces a slight input circuit delay 36 in the detection of the redundant light curtain signals 28 by the input I/O module 22. The input I/O module 22 may further contain processing circuitry that introduces additional input processing delay 37 into the processing of the redundant light curtain signals 28 including, for example, a coincidence detector detecting that the redundant light curtain signals 28 have both occurred essentially simultaneously.

[0037] Such coincidence circuitry must establish a window period during which each of the redundant light curtain signals must have a given logical state for coincidence to be detected. The window is sized to eliminate false anticoincidence detections caused by slight offset of the redundant light curtain signals 28 and this window period effectively introduces an additional delay into the signal processing.

[0038] The input I/O module 22 also has a network interface for communicating an input signal derived from the redundant light curtain signals 28 onto the backplane 16 to be received by one or more of the processor modules 20 such as provides a logic processing of the input signal. The backplane 16 and the necessary interface circuitry introduce a first network delay 38. In the present invention, an input signal will be transmitted from the input I/O module 22 repeatedly at a regular predetermined and known interval regardless of any change of state of the input signal.

[0039] Typically, the logic processing of the processor module 20 will logically combine multiple input signals to generate one or more output signals according to a stored control program. This logical combining of the processor module 20 introduces a logical processing delay 39 between receipt of the input signals by the processor module 20 and the generation of the output signals.

[0040] The output signals are again transmitted on the backplane 16 to the output I/O module 22' introducing a second network delay 40. The output signals are received by an output I/O module 22' which provides additional output processing delay 41 before providing electrical signals to output interface circuitry 34 which produces the halt signal 32 after an output circuit delay 42.

[0041] Referring to Figs. 2 and 3, each of the delays 36, 37, 38, 39, 40, 41, and 42 may be given a worst case value, based on design and/or testing and the sum of these delays has previously been used to characterize the assured response time of the safety controller 10.

[0042] The worst case delays 37 and 38 will collectively be determined a first worst case delay 44, while the worst case delays 39 and 40 will be collectively termed a second worst case delay 46, and the worst case output processing delay 41 will be termed the third worst case delay 48.

[0043] Note generally that a first average delay 50 associated with worst case delays 37 and 38 will generally be shorter than the first worst case delay 44, a second average delay 52 associated with delays 39 and 40 will generally be shorter than the second worst case delay 46, and a third average delay 54 associated with output processing delay 41 will generally be shorter than worst case delay 48. A maximum propagation delay time 55 may then be selected being less than the sum of the first, second and third worst case delays 44, 46, and 48 but more than the sum of the first, second and third average delays 50, 52 and 54. Generally the period of the repetition rate of the input I/O modules 22 will much smaller than the maximum propagation delay time 55.

[0044] Referring to Figs. 2, 3, and 4, the input I/O module 22 may include time stamp circuitry 60 determining a time 65 (shown in Fig. 3) when an input signal 76 (shown in Fig. 4) is received by the input I/O module 22 from the input interface circuitry 33 and attaching a time stamp 74 to that input signal 76. The time stamp 74 may be associated with serial digital representations of the input signals 76 transmitted on the backplane 16 as a header or trailer to the input signal 76 or as part of a multi-packet message including the input signal 76.

[0045] Referring to Fig. 4, during the processing of input signals 76, for example, such as may include redundant light curtain signals 28, a time stamp 74 will be attached to the input signals 76 forwarded to the processor module 20. As is generally understood in the art, the processor module 20 will effect a logical combination of multiple input signals 76 to produce one or more output signals 78. In the simplest case, the output signal 78 may be a Boolean combination of input signals 76 using AND, OR, NAND, NOR, and EXCLUSIVE OR operations.

[0046] In order to associate one of the time stamps 74 of the input signals 76 with the output signal 78, the processor module 20 may include a time stamp function 80 preprogrammed or programmed by the user to generate a time stamp 81 for the output signal 78.

[0047] In a simplest case, a preprogrammed set of rules may be applied to the time stamps 74 of the input signals 76 to select one of the times stamps 74 (TS1-TS3) of input signals 76 to be associated with the output signals 78 as its time stamp 81. Thus in the example of Fig. 4, three input signals 76, (IN1-IN3) may be used to produce an output signal 78 according to a functional relationship that is not shown. A simple rule may select the oldest (earliest) time stamp value TS2 of the input signals 76 as the time stamp 81.

[0048] Alternatively, a time stamp function 80 may be programmed by the user providing for more complex rules for determining the flow of time stamps. For example, as shown in Fig. 4, the user may program a rule that the lesser of time stamp TS1 and TS2 of input messages IN1 and IN2 are to be selected (per instruction 84) and that time stamp TS3 associated with input message IN3 is to be disregarded (per instruction 82). The time stamp function may exist in parallel with the control program that creates the output signal 78 from the input signals 76.

[0049] Referring to Figs. 2, 4, and 5, the output I/O module 22' may contain evaluation circuitry 64 that evaluates the time stamp 81 of a received output signal 78 to determine whether the safety controller 10 is working within its characterized propagation delay limits.

[0050] As shown in Fig. 5, the evaluation circuitry 64 monitors output signals 78 from the processor module 20 as indicated by decision block 86 to determine

whether an output signal 78 is overdue based on the time stamp 74 of the previous output signal. Because the transmission of output signals 78 by the processor module 20 is triggered by the receipt of input signals 76 by the processor module 20, this determination of decision block 86 simply compares the current time to the time stamp 74 of the last output signal 78 plus the maximum propagation delay time 55 as has been described.

[0051] If this time has expired, then the program proceeds to safety state 88 at which the output I/O module 22' assumes a safety output value selected by the user to be a safe state for possible failure. In this case, the safety output would be that of disabling the press 30. Importantly, by making use of the known repetition time of the input signals 76, the output I/O module 22' may enter a safety state 88 even before or without actual communication from the input I/O module 22. The safety state 88 is entered before the maximum propagation delay time 55 has been exceeded and no additional signal paths for providing a monitoring of the passage of the input signals 76 by the output I/O module 22' is needed.

[0052] If at decision block 86, the output signal 78 is not overdue, then the program checks to see whether a message has arrived at process block 87. If not, the program loops back to process block 86.

[0053] If an output signal 78 has arrived at time 68, then as indicated by process block 90, the time stamp 74 of the output signal 78 is stored for use by process block 86 which is then returned to for the next signals overdue comparison as has been described. .

[0054] The present invention has been described with respect to a system which provides for synchronized clocks at the input I/O module 22 and output I/O module 22'. It will be understood that synchronized clocks are not required so long as the output circuit has knowledge of the offset between the clocks of the input circuit and output circuit such as may be obtained within a predetermined accuracy by estimating offsets through a number of techniques, and subtracting the uncertainty in the offset from the predetermined time delay. For example, the input I/O module 22 and output I/O module 22' may exchange time stamped messages transmitted in both directions to net out constant propagation delay, this value may be averaged over

time to yield a clock offset to a given tolerance. The clock offset may be used to synchronize the clocks of the input I/O module 22 and output I/O module 22' and the uncertainty in this correction subtracted from the maximum propagation delay time 55 to ensure the maximum propagation time is not exceeded because of errors between clocks.

[0055] Both circuitries 60 and 64 may be implemented as software routines within a microprocessor running on the respective input I/O module 22 and output I/O module 22' or may be implemented in discrete circuitry for gate arrays as is well known in the art, or other technique.

[0056] It is specifically intended that the present invention not be limited to the embodiments and illustrations contained herein, but include modified forms of those embodiments including portions of the embodiments and combinations of elements of different embodiments as come within the scope of the following claims.